UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/750,594	12/31/2003	Ryan Charles Catherman	RPS920030206US1	8589

25299 7590 01/10/2007	EXAMINER	
IBM CORPORATION PO BOX 12195 DEPT YXSA, BLDG 002 RESEARCH TRIANGLE PARK, NC 27709	WILLIAMS, KENT L	
	ART UNIT	PAPER NUMBER
	2112	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

	Application No.	Applicant(s)
Office Action Summary	10/750,594	CATHERMAN ET AL.
	Examiner	Art Unit	
	Kent L. Williams	2112	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 December 2003*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Specification

1.   The disclosure is objected to because it contains an embedded hyperlink and/or

other form of browser-executable code. Applicant is required to delete the embedded

hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

2.   The attempt to incorporate subject matter into this application by reference to

"trustedcomputinggroup.org" in paragraph 6 is ineffective because it is browser

executable code and does not clearly reference the relevant content in relation to the

instant application. The content relied upon *may* ultimately be incorporated into the

specification without adding new matter.

3.   The attempt to incorporate subject matter into this application by reference to

"csrc.nist.gov/publications/fips" in paragraph 46 is ineffective because it is browser

executable code and the relevant content cannot be determined.

4.   The disclosure is objected to because of the following informalities: The "Related

Application" section is missing the serial number of the related application

(#10/749,261). As per section 1 (of this application), browser executable code is found

in paragraph 6, line 6 and paragraph 46, line 5. Also, "Complaint" should be "compliant"

in paragraph 7, line 2. "Require" should be "required" in paragraph 9, line 4. EEPROM

is "Electrically Erasable Programmable Read Only Memory" and not "Erasable,

Electrically Programmable Read Only Memories" as found in paragraph 52, line 7.

Within the abstract section, "TPM" should be spelled out as "trusted platform module."

"OEM (original equipment manufacturer)" should be "original equipment manufacturer

(OEM)" within claim 1. Claim 2 states "secret number (secret)" and refers to secret

number as "said secret" thereafter, but should be rewritten to read just "secret number"

and referred to as "said secret number" thereafter.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

5.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6.   Claims 1-4, 6-8, 10-15, 17-24 are rejected under 35 U.S.C. 102(b) as being

anticipated by Jean Petty, "Trusted Computing Platform Alliance (TCPA) Trusted

Platform Module Protection Profile Version 1.9.4," 15 March 2002, (referred to as Petty

hereinafter).

Due to the nature of Petty, which is an evaluation (or "protection profile") of the

"Trusted Computer Platform Alliance (TCPA) Main Specification Version 1.1b" (referred

to as TCPA hereinafter), Petty inherits all of the "Main Specification Version 1.1b" as it is

an evaluation thereof. Also, to show inherence of a few features found within TCPA and

Petty, a couple other articles that reflect on TCPA or analyze the TCPA specification will

be used per MPEP §2131.01.

Claims 1-4, 6-8, 10-15, 17-24 recite generating an endorsement key pair, generating a secure value (and secret), verification of the public key of the endorsement key pair, insertion of an endorsement certificate, supporting structures (processor, bus, etc.), EK formulation using public endorsement key and a secret hashed after concatenation, transmitting the EK to a server by secure *means*, the secret being a 1-time use parameter, and endorsement confirmation of the EK on the server by recalculation.

Petty teaches "The TSF shall restrict the ability to initialize or modify the TSF data: *Endorsement Key Pair, TPMProof* to the *TPM manufacturer* or *designee*. (Page 20, FMT_MTD.1.1;3)." This is in reference to TCPA, which teaches the use of an "endorsement key pair" (EK) (that creates the uniqueness of the TPM itself as a self-verifier and not claims of the instant application), and "TPMProof to the TPM Manufacturer" (an unspecified secret (verification means) to conclude the TPM is genuine to the OEM for certification). The Examiner is interpreting the statement that the device shall not allow modification after instantiation of the EK and the OEM "proof" (a secret), as saying that the EK and "proof" ("secret") must be injected (AKA "squirted") into the device at manufacture time. It is understood that the "proof" ("secret") must be known by the OEM's endorsement certification authority to be of any use. However, the statement only covers restriction of "initializing" and "modifying," therefore is silent of "deletion" (AKA "destroying"), which is the only viable option beyond those restricted. Therefore, Petty has shown that the TPM will be using EK and TPMProof (a "secret") to endorse the device as unique, and subsequently deleting said TPMProof after the TPM

has been endorsed via the EK (of the instant application). The Examiner finds, via

evidence shown supra, that Petty teaches generation of an endorsement key pair for

every valid device, a secure value (AKA a "secret" or "TPMProof"), verifying by means

of said endorsement key pair and secure value for use in verification for inserting an

endorsement certificate into said device. However, the Examiner understands that

deletion ("destroying") said secret upon verification and certification is <u>not</u> inherent, but

the only alternative, leaving the secret intact, does not constitute an acceptable policy of

any TPM device, as its only intended use is to verify the Endorsement key pair of the

TPM. Although, it can be argued that the process "TPM_Terminate_Handle" that is

directed to termination of a communication session, does state that: "The TPM SHALL

terminate the session and destroy all data associated with the session indicated.

(TCPA, page 114)." Please also see page 5, sections 2.2.2 through 2.2.5, and the

glossary (if necessary) of Petty for further clarification. Even further clarification can be

found on page 282, section 9.5 (and 9.5.1).

Petty was evaluating the TCPA that states, "The TPM_ReadPubek command

shall [...] 3. Create checksum by performing SHA1 on the concatenation of (PUBEK ||

antiReplay). (Page 264)." This merely states that the TPM will produce a hash of the

"secret" (AKA "antiReplay," see page 186, type "TCPA_NONCE") with the public key of

the endorsement key pair (AKA "PUBEK"). The Examiner finds that performing a hash

(SHA1) function of the data teaches securing a communication, per se. Creating a hash

using an "antiReplay" and the EKPUB is the exact same as creating a hash of the public

key of the endorsement key pair concatenated with the secured value (or secret). A

"secret" is a nonce by definition, and a nonce is a 1-time use value by definition. To

further define the above paragraph and this paragraph (of this office action), TCPA

outlines the process for creating a "New Entity" that is directed to instantiating a TPM on

page 115-117 (TCPA, §5.4, named "ADIP – Creating a New Entity"). Please note that

within "ADIP – Creating a New Entity," "the creator" is the same as the certification

authority server. Without being too convoluted in analysis, TCPA teaches the request

for an endorsement certification using a hash of a "shared secret" (page 115, paragraph

10) and the PUBEK as presented previously within this office action; and the actions for

reply of the server (transmitting the EK, verifying *means*, and subsequent insertion of

the endorsement certificate) are taught *per se* on pages 115-117. Even further

definition can be found on page 261, section 9.2. Further evaluation of TCPA by other

authors gives more simplified light on the subject matter: Sundeep Bajikar shows that

there is reason behind remote certification of the endorsement key pair apart from the

manufacturing site: "The same party that provides the EK may not provide the

Endorsement Cert. ("Trusted Platform Module (TPM) based Security on Notebook PCs

– White Paper," page 8, last line)." Also, and to reiterate points already made, "The

TPM has a key pair called the endorsement key pair that is set at the time of

manufacture. This key pair cannot be changed or erased and the private key is never

released to the outside by the TPM. A so-called TPM Entity (TPME), normally the

manufacturer, provides a certificate of the endorsement public key called the

endorsement credential. The endorsement key pair is unique to the TPM and, hence, its

use in transactions with other parties would provide a means of unambiguously

identifying the TPM.   (Reid et al., "Privacy and Trusted Computing," page 3, §3, lines 1-

9)."

The Examiner finds that a processor, bus and network interface (per claim 12),

and a processor with memory (per claim 14) is inherent within the reference as a TPM's

primary design is for use with a general-purpose personal computer that encompasses

those structures. Please also see page 3, sections 2.1 through 2.2, for further

clarification.

The Examiner wishes to convey that the nature of the previous 35 USC §102(b)

rejection is convoluted due to the convolution of Petty and TCPA. It is to be understood

that the rejection cannot be fully evaluated without a sound understanding of TCPA and

Petty, respectively. In short, the rejection, just as the two references, may be confusing.

If any part of this rejection is not understood or does not seem appropriate to the

applicant, the examiner will be willing to grant an interview to discuss any necessary

misunderstood points. However, the inventors are a good reference for better

assistance in understanding.

Double Patenting

7.   The nonstatutory double patenting rejection is based on a judicially created
doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the
unjustified or improper timewise extension of the "right to exclude" granted by a patent
and to prevent possible harassment by multiple assignees. A nonstatutory
obviousness-type double patenting rejection is appropriate where the conflicting claims
are not identical, but at least one examined application claim is not patentably distinct
from the reference claim(s) because the examined application claim is either anticipated
by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140
F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29
USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir.

1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

8.   Claims 1-25 are provisionally rejected on the ground of nonstatutory

obviousness-type double patenting as being unpatentable over claims 1-25 of

copending Application No. 10/749,261. Although the conflicting claims are not identical,

they are not patentably distinct from each other because the claimed subject matter of

both applications are directed towards certifying an endorsement key pair of a trusted

platform module by a certification authority (a server) and a secret value (that

encompasses a key or key pair). The *most* notable correlations between the instant

application and the copending application are, respectively: Claims 1, 12, 14 and 17 to

claims 1, 12, 14, 17 (certification of endorsement keys for TPM's by OEM CA); claims 9,

24 and 25 to claims 9 and 25.

This is a <u>provisional</u> obviousness-type double patenting rejection because the

conflicting claims have not in fact been patented.

9.   Claims 1-8, 10-24 are provisionally rejected on the ground of nonstatutory

obviousness-type double patenting as being unpatentable over claims 1-24 of

copending Application No. 10/735,388. Although the conflicting claims are not identical,

they are not patentably distinct from each other because the claimed subject matter of

both applications are directed towards certifying an endorsement key pair of a trusted

platform module by a server using a 1-time use secret value. Most notably claims 1, 12,

14 and 17 of the instant application correlate to claims 1, 8, 14 and 20 of the copending

application. However, all of the claimed subject matter of both applications has

correlation.

This is a <u>provisional</u> obviousness-type double patenting rejection because the

conflicting claims have not in fact been patented.

10.   Claims 1-25 are provisionally rejected on the ground of nonstatutory

obviousness-type double patenting as being unpatentable over claims 1-18 of

copending Application No. 10/248,791. Although the conflicting claims are not identical,

they are not patentably distinct from each other because the claimed subject matter of

both applications are directed towards certifying an endorsement key pair of a trusted

platform module by a server using a 1-time use secret value. Although the copending

application is directed towards a business method, that business method is the method

of the instant application written as a business method for electronic transactions. The

correlations between the instant application and the copending application are,

respectively, claims 1, 12, 14 and 17 to claims 1, 4, 7, 10, 13 and 16 (certification of

endorsement keys for TPM's by OEM certification authority).

This is a <u>provisional</u> obviousness-type double patenting rejection because the

conflicting claims have not in fact been patented.

Allowable Subject Matter

11.   Claims 5, 9, 16 and 25 are objected to as being dependent upon a rejected base

claim, but would be allowable if rewritten in independent form including all of the

limitations of the base claim and any intervening claims, and also overcoming the

double patenting rejections. These claims are directed to: secrets per device correlation

to either time or quantity, limiting endorsement key pair certification failure attempts, and

a server database containing the secrets and public endorsement keys (an inherently

necessary inclusion). The novel ideas of claims 5, **9**, **16** and **25** *might* render the

invention as unique apart from the TPM specification, giving it a more secure aspect

from competitors TPM's.

Conclusion

12.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure. U.S. Patent Application Publication No. 2005/0138423 (App.

#10/745,729) is not directed toward the instant application, but claims 5 and 6 are

directed towards the instant application. All of the non-patent literatures included are

valid as previously stated. Please note the few Patents and Application Publications

directed towards TPM's based on the TCPA, and most notably Patent No. 6,185,678.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kent L. Williams whose telephone number is 571-272-1376. The examiner can normally be reached on Mon-Fri 7:00-4:30 with Alternate Fridays Off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Walter Griffin can be reached on 571-272-1447. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Kent Williams
1/05/2007

UYEN LE
PRIMARY EXAMINER